March 30, 2000

Brigadier General Thomas F. Gioconda
Acting Deputy Administrator
for Defense Programs
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0104

Dear General Gioconda:

In a letter dated November 9, 1999, the Defense Nuclear Facilities Safety Board (Board) advised you that the replacement hydrogen fluoride system being installed at the Oak Ridge Y-12 Plant to enable renewed enriched uranium metal production merited additional scrutiny. Past reviews by the Board's staff indicated that the system as designed and constructed may be lacking in features and quality commensurate with the hazards of the operations and the safety that must be ensured. Key components of the system appear to have been designed and constructed without incorporating appropriate design requirements for safety.

The enclosed report resulting from a recent review by the Board's staff reinforces these previous observations. Considering the hazardous nature of hydrogen fluoride and the processes involving its use, with the potential risk to public health and safety, special and particular attention to details of safe operation of the system seems appropriate. Such special and particular attention would include, for instance, very careful examination of the design, construction, operating characteristics, and failure modes of the system. The enclosed report highlights some issues that require attention to improve the safety of the system and to improve the ability of operators to respond to an upset condition or emergency. The design and operating characteristics of the instrumentation and control system deserve special scrutiny.

The Board plans to be at Y-12 in April and looks forward to a briefing at that time from the Department of Energy on the adequacy of the safety basis of the hydrogen fluoride supply system and on the design requirements for associated safety-significant systems.

Sincerely,

John T. Conway
Chairman

c: Mark B. Whitaker, Jr.
Ms. Gertrude Leah Dever

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

March 10, 2000

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: W. White

SUBJECT: Instrumentation and Control for Hydrogen Fluoride Supply System

This report documents a review performed December 15–16, 1999, at the Oak Ridge Y-12 Plant by members of the staff of the Defense Nuclear Facilities Safety Board (Board). Staff members W. White and D. Moyle met with Lockheed Martin Energy Systems (LMES) personnel to discuss the instrumentation and control systems for the hydrogen fluoride (HF) supply system. The staff also conducted a video conference with Department of Energy (DOE) and LMES personnel on January 28, 2000, and performed reviews of related documents during February 2000 to follow up on issues raised during the December review.

Instrumentation and Control Systems for HF Supply System. In reviewing the safety-significant instrumentation and control systems for the HF supply system, the staff considered carefully the potential impacts of postulated accidents. According to LMES personnel, the worst-case, off-site release of HF in an accident situation is 1000 parts per million, which is more than 30 times the level considered immediately dangerous to life and health.

It was not clear to the staff why controls designed to prevent such serious off-site consequences were not safety-class. The staff is currently following up on this issue with LMES. Given the off-site consequences, the staff expected to see stringent design criteria for HF safety systems, whether they are classified as safety-class or safety-significant. According to LMES personnel, however, no process industry, nuclear industry, or DOE standards were used to provide design criteria for the safety-significant instrumentation and control systems.

As discussed in previous Board letters and staff reports on instrumentation and control systems at Oak Ridge (November 4, 1997), Los Alamos National Laboratory (September 22, 1999), Lawrence Livermore National Laboratory (December 21, 1999), and the Savannah River Site (SRS) (December 22, 1999), this problem appears to exist across DOE's defense nuclear complex. Some sites, however, have begun to consider the use of process industry safety standards (e.g., Instrument Society of American [ISA] Standard S84.01, *Application of Safety Instrumented Systems for the Process Industries*) for the design of safety-significant systems, where appropriate. As the Board and its staff have noted in previous reports, the use of industry standards could significantly improve the design of safety-significant systems.

Considering the potential off-site consequences of HF releases, and given the absence of safety-related design criteria, the staff noted several areas for improvement in the design of the safety-significant instrumentation and control systems for the HF supply system at the Y-12 Plant:

- In at least two cases, LMES chose to perform safety-related functions with the basic process control system, which is not designated as safety-related and was not designed, procured, or installed to standards applicable to safety-class or safety-significant systems. This basic process control system consists of programmable logic controllers that are operated through a personal computer running Wonderware® software, a standard industrial interface for process control.

  - According to the latest draft of the Limiting Conditions of Operation (LCOs) reviewed by the staff, certain process parameter values require immediate operator action to shut down the HF supply. In at least one case, these parameters are normally read only through the Wonderware® interface. The required operator actions are performed by initiating commands to the programmable logic controllers through the same Wonderware® interface. It might be prudent for LMES to consider safety-significant, hard-wired interlocks to provide the required shutdown function.

  - The reset function for the safety-significant interlocks is provided solely through the programmable logic controllers.

- The same field devices (e.g., valves) and sensors used for safety-significant emergency shutdown functions are also used for normal process control. In general, it is prudent to use separate components for the safety-significant system. Doing so provides some degree of redundancy, as well as separation from failures affecting normal process control. In fact, industry standards (e.g., ISA Standard S84.01) normally require such separation for safety systems intended to prevent serious off-site consequences.

- The power supply to certain 24 volt sensors is separate from the power supply for the interlocks and field devices. Some safety-significant sensors are not fail-safe, and loss of their power supply could result in loss of their safety-significant function. LMES might wish to consider a safety-significant power source for all sensors that do not fail in a safe condition upon the loss of power.

- LMES was unable to provide the staff with any information on the seismic qualification of safety-significant instrumentation and control systems.

- Emergency shutdown buttons (E-SCRAM) provided for personnel in HF process areas do not isolate all potential sources of HF leaks, only those considered most likely. Given the serious consequences of any HF leak, it would be prudent to interlock these shutdown buttons with all HF isolation devices. In addition, it would be prudent for LMES to consider a hard-wired solution (such as interlocking the power supply to fail-safe isolation valves), instead of implementing the emergency shutdown buttons through the programmable logic controllers.

- LMES personnel have not conducted a human factors analysis of the personal computer interface (Wonderware®) used for operation of the HF supply system. Although the system is not safety-significant, it does, as discussed above, play an important role in the response to certain LCOs. A human factors analysis could provide significant improvements in areas such as alarm management. Such an analysis might also point to the need for more rigorous requirements for operator action; currently, only a single mouse click is needed for an operator to manipulate system equipment. Accidental operation of process equipment could lead to undesirable consequences, as seen in recent occurrences at other DOE sites (e.g., shutdown of a safety-class exhaust fan at the Defense Waste Processing Facility). In fact, in conducting a human factors analysis for the operator interface of the HF supply system, LMES might wish to consider carefully the lessons learned from other DOE sites (e.g., SRS) that operate computer-based process control systems.

- LMES does not currently plan to procure a high-fidelity simulator for operator training and platform development. Given the obvious benefits of providing initial training for operators, subsequent refresher training, and testing of interface modifications on a simulator rather than operable equipment, it would be prudent for LMES to reevaluate this decision.